PERFORMANCE AUDIT

DEPARTMENT OF REVENUE
COMPREHENSIVE CONTINUITY PLANNING

From The Office Of State Auditor
Claire McCaskill

The department has limited assurance critical business processes and information systems processing functions can be resumed promptly in the event of a disruption to normal business operations.

Report No. 2002-85
September 4, 2002
www.auditor.state.mo.us

Office of
Missouri State Auditor
Claire McCaskill

September 2002

YELLOW SHEET

Department of Revenue could improve plans to recover business operations after a disaster or significant disruption

This audit analyzed the Department of Revenue's capability to resume normal business operations and recover information from automated data systems after a disaster or other disruptive event. Auditors examined disaster recovery planning, staff emergency response training, as well as testing and documentation procedures for backup systems and environmental controls. In the last year, department officials began to develop and implement a continuity plan. Audit results identified areas to enhance this plan.

Some key elements of recovery plans are complete

The department does not have a documented business continuity plan or an information technology recovery plan. As of May 2002, department officials had completed 3 of 10 key steps included in standard recovery plans. Department officials said the current preparedness level is well ahead of other state agencies, but acknowledge a comprehensive plan is far from being complete. (See pages 3 and 6)

Lack of management team and staff training impact preparedness

The department does not have an emergency management team to determine how to support overall data recovery across all business functions. In addition, department personnel are not trained in their specific roles and responsibilities regarding emergency response and business function recovery procedures. The department's formal policies for emergency fire, water, and alarm incidents also lack procedures directly related to the informational technology staff and the computer rooms. (See page 7)

Backup and off-site storage do not ensure data recovery

The department's backup, offsite storage and recovery procedures for all systems and data are not documented and in some cases are not adequate, such as storing some backup data at an employee's personal residence. The department has not tested backup systems or data to ensure they can be recovered after a disaster. (See page 8)

Environmental controls weaknesses exist

Auditors identified weaknesses in the department's environmental controls including: computer facilities not strategically placed to reduce environmental risks, inadequate documentation and testing of controls, improperly inspected fire extinguishers, no controls monitoring humidity and temperature in computer facilities, computer equipment not protected from static electricity, uninterruptible power supplies not formally tested, and no documentation of emergency evacuation plan testing results. These weaknesses put critical information technology resources at risk to environmental hazards. (See page 9)

Reports are available on our web site: www.auditor.state.mo.us

DEPARTMENT OF REVENUE
COMPREHENSIVE CONTINUITY PLANNING

TABLE OF CONTENTS

CLAIRE C. McCASKILL
Missouri State Auditor

Honorable Bob Holden, Governor
and
Carol Russell Fischer, Director
Department of Revenue
Jefferson City, MO 65102

The State Auditor's Office audited the Department of Revenue's comprehensive continuity planning preparedness. Such planning ensures business and information systems continue functioning in the event of major or minor operational disruptions. Currently, no state guidelines establish the need or specific parameters for such planning.

The objectives of this audit were to evaluate (1) whether department officials have defined and implemented a continuity planning framework, (2) whether department officials have developed and implemented a comprehensive continuity plan, including a business continuity plan and an information technology recovery plan, (3) the department's backup policies and procedures, and (4) the department's controls against environmental factors.

We concluded the department needs to develop a comprehensive continuity planning framework, including standards and policies for the development and maintenance of comprehensive business continuity and information technology recovery plans. Although the department's information technology project manager is currently involved in comprehensive continuity planning, we concluded all issues have not been addressed. Besides addressing those issues, the department also needs to test backup files to ensure they would restore critical data files in the event data is lost. Given the current level of preparedness, there is limited assurance the department could promptly resume business processes and information system processing functions in the event of a business operation disruption.

The audit was conducted in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such tests of the procedures and records as were considered appropriate under the circumstances.

Claire McCaskill

Claire McCaskill
State Auditor

The following auditors contributed to this report:

Director of Audits:	William D. Miller, CIA
Audit Manager:	Jon Halwes, CPA, CGFM
Information Systems Audit Manager:	Jeff Thelen, CPA
In-Charge Auditor:	Tara Shah, CPA
Audit Staff:	Frank Verslues

RESULTS AND RECOMMENDATIONS

Recovery Planning Needs Improvement

The Department of Revenue (department), which operates as the state's central revenue collection agency, needs better preparation to prevent a significant interruption of business operations. The department is at risk for major disruptions because department officials have not:

- Completed a comprehensive continuity plan.

- Documented (1) procedures for backup, offsite storage and recovery for computer systems and data or (2) environmental controls.

- Tested recovery of backed up systems and data or the adequacy of environmental controls.

Without continuity planning, there is no assurance normal business operations and information technology processing could be promptly resumed in the event of a disaster or other disruptive event. Testing recovery of back up applications and data as well as testing the adequacy of environmental controls is also critical to limit interruptions and minimize the impact of any disruption to operations. Due to the department's role in revenue collection, it is important critical business operations remain functioning or can be resumed promptly with the least possible disruption. The department's information technology project manager is currently involved in comprehensive continuity planning; however, all issues have not been addressed. Department officials believe their current level of preparedness is well ahead of other state agencies, but acknowledge a comprehensive continuity plan is far from complete.

Description of comprehensive continuity planning

An organization must take steps to ensure it is adequately prepared to cope with a loss of operational capability. An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. There are three main classes of events that might affect an organization's ability to continue business operations; an unplanned incident or accident such as an explosion or fire, a natural cause disaster such as a tornado or earthquake, or a deliberate act to disrupt the operations of a business, government, institution, or some other organization.

An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested continuity plan. Comprehensive continuity planning encompasses both business continuity and information technology recovery. With business continuity planning, an organization is ensuring the availability of all business resources and supporting information technology needs to continue/resume business processes. For information technology recovery planning, the organization is ensuring the availability of information technology resources required to support the continuity or recovery of business processes. A comprehensive continuity plan specifies emergency response, backup operations, and restoration procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. It addresses how an organization will deal with a full range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a continuity plan should be periodically tested in disaster simulation exercises and employees should be trained in and familiar with its use.

Criteria used to evaluate the department's comprehensive continuity planning

There are currently no state regulations requiring agencies to develop, implement, and maintain a comprehensive continuity plan. However, there are federal standards as well as national and international standards related to comprehensive continuity planning. For our review of comprehensive continuity planning, accepted standards from the following sources were used:

- National Institute of Standards and Technology
- American Institute of Certified Public Accountants
- Canadian Institute of Chartered Accountants
- Information Systems Audit and Control Association
- United States General Accounting Office

The department has three divisions (Motor Vehicle and Drivers Licensing, Taxation and Collection, and Administration). Each of these divisions has an administrator of technology services who reports to his/her respective division director. The department also has a chief information officer who handles department-wide issues and works with all the divisions. In addition, the State Data Center operates as a contract service provider to the department. The data center provides mainframe data processing and facilitates the storage of data and backups for the department.

The department is directly responsible for the collection of taxes and motor vehicle registration and drivers licensing fees. Approximately 118 computer applications are used by the staff to support the department's operations. The total state revenue for fiscal year 2001 was approximately $17 billion. Besides the impact on state government operations, a significant business interruption could seriously impact city and other local government operations due to the department's role in collection and distribution of local sales tax revenue.

Department officials indicated they have evaluated continuity planning and security over the last several years and were one of the first state agencies to discuss these issues with State Data Center officials. Efforts were started in the last year to put a comprehensive continuity plan in place.

Plans are needed for resuming critical business operations and system processing

The department does not have a documented business continuity plan or an information technology recovery plan. In September 2001, department officials hired an information technology project manager to develop a comprehensive continuity plan, which would integrate business continuity and information technology recovery plans. The project manager is developing the plans based on information obtained from training sessions and his own knowledge. He is not using standards from any of the sources noted on page 4. His main focus is developing a business continuity database, which is being constructed through responses from suppliers and users of the department's operations. He indicated this database is the focal point of the initial work, because it is the basis for the plan that will be put in place. As of May 2002, the database has been used to document business applications and operations as well as prioritize the applications; however, not all applications and operations have been identified. Maximum business and system outage tolerance[1] and restoration time periods are also being identified and included in the database. For example, the dealer registration system administered by the Division of Motor Vehicle and Drivers Licensing was determined to have an outage tolerance of 2 to 4 weeks with an estimated restoration time of less than 1 week. Only 20 percent (24 of 118) of the department's applications are assigned an outage tolerance with only 18 applications assigned an estimated restoration time. The estimated restoration time for two applications exceeded the outage tolerance identified.

Project manager developing continuity plan

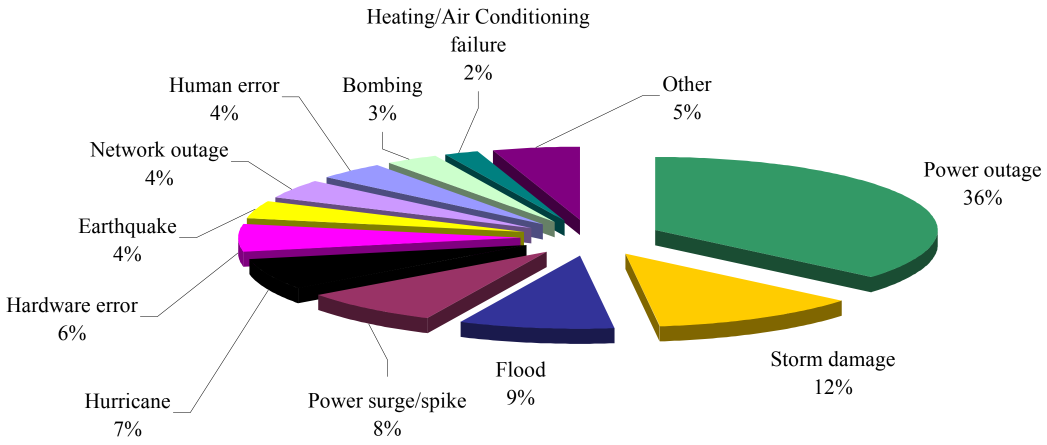
Although the department's management could, through use of this partially completed database, determine the functions, applications, personnel, and equipment impacted by a disaster, there is still no assurance the department could promptly resume business operations. A comprehensive continuity plan will help the department ensure timely resumption of operations and recovery of data in the event of a disaster or other disruptive event.

A recent national study showed 43 percent of companies which experience a major disaster and do not have an adequate continuity plan do not re-open, while 29 percent are out of business within 2 years. The overall survival rate without a plan is 28 percent.[2] While the department could not cease to exist, the length of time critical operations may not be functioning could severely impact the state. Figure 1.1 shows a breakdown of the most common causes of disruptions.

[1] Maximum time a system or operation could be shutdown before impacting a business.

[2] *Business Continuity Management In Today's Environment,* a seminar presented to the St. Louis Chapter of the Institute of Internal Auditors on October 25, 2001 by Jefferson Wells International.

Figure 1.1: Types of Disruption



Source: *Business Continuity Management In Today's Environment,* a seminar presented to the St. Louis Chapter of the Institute of Internal Auditors on October 25, 2001 by Jefferson Wells International.

According to accepted standards,[3] continuity plans should:

- Be documented and approved by senior management.
- Identify all critical business applications and operations.
- Prioritize the critical business applications and operations.
- Identify resources needed to support critical functions.
- Satisfy the established maximum outage time periods.
- Include network infrastructure issues.
- Implement parallel processes where appropriate.
- Address disasters of varying degrees.
- Include alternate processing facility agreements.
- Be periodically tested to ensure they are kept relevant and effective.

At the end of our fieldwork, department officials had completed items 2, 3 and 4 on the above list.

Organizational policies should require a continuity planning framework to ensure consistency in continuity plans and to ensure all necessary items are included in the plan. This framework should be a part of normal operational requirements and function as an outline guiding the planner to the general issues needing to be documented in the plan. The department's information technology project manager will be developing a framework for the comprehensive continuity planning process. The framework will define the roles, responsibilities, and the risk-based approach/methodology to be adopted, the rules and structures to document the plan, and the approval procedures.

[3] Standards established by the five organizations identified on page 4.

Department planning needs to consider additional areas

Our review of the continuity planning that has taken place since September 2001, indicate the following weaknesses have not been addressed and were not being sufficiently considered:

- No emergency management team.
- Lack of emergency response training for personnel.
- Inadequate procedures to analyze the impact of various disruptive events.
- Lack of emergency response procedures for information technology staff.
- Weak and untested backup, and recovery procedures.
- Weak and untested environmental controls.

Management team and personnel training would improve recovery preparedness

The department does not have an emergency management team to develop consolidated strategies for overall information technology recovery support across all business functions. Currently, each division has an administrator of information technology who would work with the information technology project manager to coordinate recovery activities. Therefore, in the midst of a disaster, the department would lack the consolidated input and cooperation of a management team to implement appropriate recovery strategies. This weakness could result in the department losing valuable time in the assessment and recovery phases of a disaster. For employees to respond in an orderly fashion, accepted standards suggest that an emergency management team or similar function be assigned the responsibility to determine whether to activate continuity plans and coordinate recovery activities.

Department personnel are not trained on their specific roles and responsibilities relating to emergency responses and business function recovery procedures. Personnel have responsibilities to uphold in the event of a disaster. Without such guidance and training, department management cannot ensure personnel will react properly to a disaster and be able to effectively and efficiently carry out their responsibilities.

Management needs to evaluate the impact of risks or threats

The department does not have procedures to analyze the impact of various disruptive events. According to accepted standards, updating potential risks and exposures should be an ongoing risk management activity. A business impact analysis would consider different types of risks and threats and their corresponding impact on business functions. Potential business interruptions as well as maximum tolerable down times should be identified for all critical business functions. This analysis will allow management to identify how long a critical function may be out, the impact on other business functions if it is out longer than anticipated, and what alternatives should be considered to resume business operations.

Impact analysis would improve decision process

Various strategies are available for recovering business operations. The appropriate strategy is the one that balances preventive, recovery, and restoration measure costs against the business and operational impact of possible outages and likelihood of occurrence. This business impact analysis would allow management to select the most appropriate alternative to resume business operations based on the relative risks identified.

Emergency response plans have not been developed

Although the department has formal policies for emergency fire, water, and alarm incidents, these policies lack procedures outlining responsibilities of information technology staff and procedures directly related to the computer rooms. Accepted standards call for emergency response plans to be developed in advance to manage business recovery activities and information technology recovery activities.

Due to the centralized nature of information technology processing activities, there is a higher degree of risk of potentially disruptive events in computer operation areas than in other parts of the department. There are unique physical security and access requirements for computer operation areas relating to premises evacuation, life and health safety of employees and others, damage mitigation and containment, and preliminary damage and impact assessment. The department has not developed emergency response plans for information technology operations and cannot ensure the safety of employees or prepare the department for immediate response to an emergency.

Backup and offsite procedures are not documented

The department's backup, offsite storage and recovery procedures for all systems and data are not documented and in some cases are not adequate. The department has not tested backup systems or data to ensure they would properly restore systems and data in the event of a disaster. As a result, critical data may not be recoverable in the event of system failures. Backup and recovery procedures are a critical component of the information services function and help ensure continued operations.

Backup systems have not been tested

Accepted standards state that backup and off-site storage plans should:

- Document backup procedures for data files and software.
- Document procedures for off-site storage, or availability of all material which would be required to restore and recover critical business functions within their identified maximum outage time periods.
- Ensure appropriate retention cycles have been established for critical off-site storage documentation based on the business needs and risks.
- Require periodic testing of off-site backup files to ensure the material required to resume/recover critical business processes are available.
- Ensure information technology staff and division managers have approved backup and off-site storage procedures.
- Document procedures for restoring from backup.

Auditors noted five weaknesses in the department’s current backup procedures which include (1) lack of assignment for the control of offsite storage of data files to a librarian, (2) failure to base backup application and data retention cycles on business needs, (3) lack of a perpetual inventory of backup tapes and other secondary storage media, (4) inadequate use of physical and/or environmental controls[4] to protect data, and (5) lack of segregation of duties. For example, a manager in one division is responsible for performing the backup of the network and also for storing the backup tape offsite at her home. In this instance, the same person is creating the backup tape and controlling the tape in her home which is not a secure environment.

Critical resources and operations could be at risk to environmental hazards

There are environmental control weaknesses in the department. Although department officials rely heavily on the environmental controls implemented, maintained, and tested by the Office of Administration, the department is responsible for additional controls. The following weaknesses in the department's environmental controls were noted:

- The computer facilities were not strategically placed to reduce environmental risks such as air temperature. Rather, the server rooms were selected as to which rooms were available at the time.
- Controls in place are not adequately documented or tested.
- The fire extinguishers are not properly inspected.
- There are no controls to monitor humidity and temperature of the computer facilities.
- Computer equipment is not protected from the effects of static electricity.
- The uninterruptible power supplies are not formally tested.
- The results of emergency evacuation plan testing are not documented.

As a result, critical information technology resources could be at risk to environmental hazards, which could easily harm or destroy the resources and systems responsible for supporting critical business operations. According to accepted standards, adequate environmental controls should be in place and documented. In addition, there should be procedures in place for testing environmental controls to help mitigate the risk of disaster (ie. fire, flood, tornados, earthquakes, and power outages). Environmental controls can diminish the losses from some interruptions or detect potential problems early.

Conclusion

Department operations face significant risks without a completed comprehensive continuity plan, adequately documented and tested backup and recovery procedures, and adequately documented and tested environmental controls. Department officials recognize these issues and have begun to address them, but more needs to be done to ensure operations can resume promptly in the event of a disaster or other disruptive event.

[4] Smoke detectors, fire alarms and extinguishers, humidity and temperature controls, and uninterruptible power supplies are some examples of environmental controls.

Recommendations

We recommend the Director, Department of Revenue:

1.1 Define and implement a continuity planning framework, including standards and policies for the development and maintenance of comprehensive business continuity and information technology recovery plans. Ensure this framework includes provisions to:

- Assign the responsibility of coordinating disaster recovery and business resumption activities to an emergency management team, and ensure all personnel are aware of and trained in their duties and responsibilities as they apply to the comprehensive continuity plan.

- Develop formal procedures to incorporate periodic business impact analysis to monitor the ongoing requirements of the business continuity plans and arrangements.

- Develop and document adequate emergency response procedures regarding information technology recovery activities, and ensure staff are appropriately trained on how to respond in the event of an emergency.

1.2 Develop, implement, and maintain a comprehensive continuity plan, which consists of both a business continuity plan and an information technology recovery plan. Once the plans are implemented, they should be periodically tested.

1.3 Develop and document backup, recovery, and offsite storage procedures for critical data files, applications, media, documentation, and other information technology resources to support the recovery and resumption of business processes and system operations. These procedures should include policies to test recovery of backup applications and data, use of a librarian to track backup data, perpetual inventories of backup data and media in secondary storage, segregation of duties for personnel responsible for creating backup data, and proper storage of backup data.

1.4 Evaluate the adequacy of environmental controls in place and test the controls periodically.

Department of Revenue Responses

1.1 The department agrees that a framework for the development of a comprehensive business continuity plan should be implemented. The framework provided in ISO 17799 (International Standard 17799, Information Technology - code of practice for information security management) provides the standards to be used in the development, testing, and maintenance of the department's Business Continuity Plan. As recommended, the execution of any business continuity activities or information technology disaster recovery activities will ultimately reside with an emergency management team. Additionally, procedures will be included to ensure a formal process *for periodic business impact analysis to monitor and provide for a plan, which is viable for existing operations.*

1.2 *The department agrees that a comprehensive Business Continuity Plan and Information Technology Disaster Recovery Plan should be developed. The department is currently developing such plans in accordance with the framework established in ISO 17799.*

1.3 *The department agrees that our backup, recovery, and offsite storage procedures for critical data, files, applications, media, documentation, and other information technology resources could be better documented. Following recent recovery tests and efforts related to disaster recovery planning, documentation and procedural changes are being discussed and evaluated for implementation.*

1.4 *The department agrees that environmental controls should be tested to ensure their adequacy. Procedural changes are being discussed and evaluated for implementation.*

APPENDIX I

OBJECTIVES, SCOPE AND METHODOLOGY

Objectives

The objectives of this audit were to evaluate (1) whether department officials have defined and implemented a continuity planning framework, (2) whether department officials have developed and implemented a comprehensive continuity plan, including a business continuity plan and an information technology recovery plan, (3) the department's backup policies and procedures, and (4) the department's controls against environmental factors.

Scope and Methodology

Auditors conducted fieldwork during April and May 2002. The audit included:

- Review of applicable federal, national and international standards related to comprehensive continuity planning.
- Discussion with department personnel involved in comprehensive continuity planning.
- Review of work-in-process data from the department's information technology project manager.

The audit reviewed the department's practices and procedures for business continuity except for activities that are the responsibility of the State Data Center. Therefore, our audit did not review the controls of the State Data Center related to the department's ability to recover applications or files after a significant disruption to business operations.

APPENDIX II

DEFINITION OF TERMS

Some key terms and definitions accepted by the organizations noted on page 4 that have developed national and international standards for comprehensive continuity planning include:

Business Continuity: The discipline of planning for the recovery of business operations in the event that normal business resources, such as office space, terminals, microcomputers, office machines, terminals and networks, are made unavailable following a disaster. The term normally does not include the separate, but closely related, discipline of disaster recovery planning for information technology resources.

Disaster Recovery: The discipline of planning for the recovery of information technology operations in the event that normal operations are made unavailable as a result of a disaster; normally, closely related to the discipline of business continuity planning.

Application: Any of a class of "programs" or "software", which causes a computer to perform some useful function such as data entry, update or query.

Emergency Response: Encompasses the initial actions taken to protect lives and limit damage.

Environmental Control: Controls which prevent or mitigate damage to facilities and interruptions in service due to environmental hazards. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls.

Framework: An outline of the issues which need to be addressed in the comprehensive continuity plan.

Recovery: The ability to resume processing without irreparable loss of system data after an error or malfunction in software or hardware.

APPENDIX III

REFERENCES

American Institute of Certified Public Accountants

AICPA/CICA SysTrust: Principles and Criteria for Systems Reliability, Version 2.0, January 2001.

Auerbach Publishers

Information Technology Control and Audit, Frederick Gallegos, Daniel P. Manson and Sandra Allen-Senft, 1999.

Standard for Auditing Computer Applications, Martin A. Krist, 1999.

Canadian Institute of Chartered Accountants

Information Technology Control Guidelines, 3rd Edition, July 1998.

Federal Chief Information Officers Council

Federal Information Technology Security Assessment Framework, November 28, 2000, http://www.cio.gov.

Information Systems Audit and Control Foundation

Control Objectives for Information and Related Technology (COBIT), 3rd Edition, July 2000, http://www.isaca.org.

Certified Information Systems Auditor (CISA) Review Manual, 2002, http://www.isaca.org.

National Institute of Standards and Technology

Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995, http://csrc.nist.gov.

Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996, http://csrc.nist.gov.

Special Publication 800-18, *Guide For Developing Security Plans For Information Technology Systems,* December 1998, http://csrc.nist.gov.

Special Publication 800-26, *Security Self-Assessment Guide For Information Technology Systems,* November 2000, http://csrc.nist.gov.

U.S. Office of Management and Budget

Appendix III to OMB Circular No. A-130, *Security of Federal Automated Information Resources*, November 2000, http://www.whitehouse.gov/omb/circulars/index.html.

U.S. General Accounting Office

Federal Information System Controls Audit Manual: GAO/AIMD-12.19.6, January 1999, http://www.gao.gov.

Warren Gorham & Lamont/RIA Group

Handbook of IT Auditing, 2001 Edition.